IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., by and through next friend, LILIANA T. HANLON, SHIMERA JONES, LEROY JACOBS, BALARIE COSBY-STEELE, JOHN DEMATTEO, RICHARD MADAY, ALLISON THURMAN, and SHERIE HARRIS, individually and on behalf of all others similarly situated,	)	Case No. 1:21-cv-04976
Plaintiffs,	)	Hon. Lindsay C. Jenkins Presiding Judge
v.	)	
SAMSUNG ELECTRONICS AMERICA, INC., and SAMSUNG ELECTRONICS CO., LTD.	)	
Defendants.	)	

CONSOLIDATED SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs G.T., a minor by and through next friend Liliana T. Hanlon, Shimera Jones, Leroy Jacobs, Balarie Cosby-Steele, John DeMatteo, Richard Maday, Allison Thurman, and Sherie Harris (collectively, "Plaintiffs") individually and on behalf of all other persons similarly situated, bring this class action lawsuit for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*., against Defendant Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd., (collectively, "Samsung"). Plaintiffs allege the following facts based on personal knowledge, investigation by counsel, and on information and belief where indicated.

NATURE OF THE ACTION

1. Plaintiffs bring this Amended Class Action Complaint on behalf of Illinoisans harmed as a result of Samsung's surreptitious capture, collection, use, and storage of their highly

sensitive biometric identifiers[1] and biometric information[2] (collectively or separately, "Biometrics").

2. Samsung is the designer, manufacturer, and vendor of Samsung smartphones and tablets ("Devices"), the most popular of which include the Galaxy smartphones and the Galaxy Tab tablets. Samsung has nearly 30% of the smartphone market in the United States and 17.6% of the tablet market, having sold more than two billion Galaxy smartphones since 2009 and over 50 million Galaxy Tab tablets in the past two years alone.

3. All Samsung Devices are manufactured and sold with the Gallery application ("Gallery App") pre-installed as the default photograph and video application. All photos added to the user's Device are automatically saved to the Gallery App.

4. Unbeknownst to users, Samsung uses facial recognition technology on each photograph saved to the Gallery App. Samsung's algorithm automatically scans and analyzes each image to determine whether a face is present. Once a face is detected, the algorithm analyzes and extracts a scan of the person's unique facial geometry and uses artificial intelligence to create a unique digital representation of it known as a "face template."

5. Each face template is stored in a facial recognition database on, at least, the user's Samsung Device in the solid state memory, and then accessed and compared against each newly-stored face template to determine whether there is a match.

6. This entire process is automated without the user's involvement or consent whenever a new photograph is added on a Samsung Device. Users cannot disable this facial recognition technology, nor can they prevent Samsung from harvesting Biometrics from the faces

[1] A "biometric identifier" is any personal feature that is biologically unique to an individual, such as retina scans, fingerprints, and scans of face geometry. 740 ILCS 14/10.

[2] "Biometric information" is any information based on a person's biometric identifier used to identify an individual. 740 ILCS 14/10.

in photographs stored on their Samsung Devices.

7. Instead of disclosing its practice of collecting biometric identifiers in the form of faceprints and face scans, Samsung intentionally deceives users into believing that Samsung applies non-facial recognition processes by disclosing what it calls an "image analysis," while failing to notify users that this system cannot function without repeatedly capturing scans of their facial geometry and using it to generate face templates.

8. Samsung does not notify Illinois users Samsung is generating, collecting, using, and storing their biometric information and biometric identifiers.

9. Samsung does not disclose its biometric data collection to its users, nor does it ask users to acknowledge, let alone consent to, these practices.

10. Through these practices, Samsung not only disregards the users' privacy rights; it also violates the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which was specifically designed to protect Illinois residents from practices like Samsung's. In particular, Samsung violated (and continues to violate) BIPA because it does not:

- Properly inform Plaintiffs or the Class in writing their Biometrics (faceprints and face scans) were being generated, collected, or stored;
- Properly inform Plaintiffs or the Class in writing of the specific purpose and length of time for which their Biometrics were being collected, stored, and used;
- Receive a written release from Plaintiffs or the Class to collect, capture, or otherwise obtain their Biometrics.
- Maintain and adhere to a publicly-available written policy setting forth its retention schedules and guidelines for permanently destroying Biometrics.

11. Accordingly, this Complaint seeks an order (i) declaring that Samsung's conduct violates BIPA; (ii) requiring Samsung to cease the unlawful activities discussed herein; and (iii) awarding statutory damages to Plaintiffs and the proposed Class.

PARTIES

Plaintiffs

12. Plaintiff G.T., a minor, is a natural person and citizen of Illinois. Liliana T. Hanlon, G.T.'s next friend, is a natural person and citizen of Illinois.

13. Plaintiff Shimera Jones is a natural person and citizen of Illinois.

14. Plaintiff Leroy Jacobs is a natural person and citizen of Illinois.

15. Plaintiff John DeMatteo is a natural person and citizen of Illinois.

16. Plaintiff Balarie Cosby-Steel is a natural person and citizen of Illinois.

17. Plaintiff Richard Maday is a natural person and citizen of Illinois.

18. Plaintiff Allison Thurman is a natural person and a citizen of Illinois.

19. Plaintiff Sherie Harris is a natural person and a citizen of Illinois.

Samsung

20. Defendant Samsung Electronics America, Inc. ("Samsung America") is a New York corporation with its principal place of business at 85 Challenger Road, Ridgefield Park, New Jersey.

21. Samsung America is a wholly-owned subsidiary of Defendant Samsung Electronics Co., Ltd. (f/k/a Samsung Electronic Industries). Samsung America is responsible for the sale of Samsung devices in the United States.

22. Defendant Samsung Electronics Co., Ltd. (f/k/a Samsung Electronic Industries) ("Samsung Electronics"), is a South Korean multinational corporation headquartered in the Yeongtong District of Suwan, was incorporated under the laws of the Republic of Korea in 1969 and lists its shares on the Korea Stock Exchange in 1975. Samsung Electronics Co., Ltd. is the parent company to Samsung Electronics America, Inc.

23. Samsung Electronics is responsible for manufacturing Samsung Devices, including mobile phones.

24. Samsung America and Samsung Electronics conduct significant business throughout the State of Illinois and the United States, including through the manufacturing, sale, and shipment of Samsung Devices.

25. As of December 31, 2021 Samsung earned more from the United States than any other region in the world, bringing in a total net revenue of approximately $68 billion. By comparison, Samsung brought in only $35 billion from Europe and even less from everywhere else, including Korea, Asia, Africa, and China.

26. In addition to device manufacturing and sales, Samsung operates "Samsung Research" which it refers to as an "advanced R&D hub" of Samsung Electronics with a focus on creating technologies for Samsung's products and services. Samsung Research focuses particularly on artificial intelligence and data intelligence, including using advanced data analytics to turn data into intelligent knowledge that will enable the ability to make inferences. Samsung Research has at least one location in the United States.

27. A subset of Samsung Research is the Samsung Research AI Center ("SAIC"), which was established in November 2017. SAIC consolidates Samsung's AI-related research terms with the company's R&D Center. SAIC operates two AI Centers in the United States. The Head of Samsung's AI Center is Daniel D. Lee, who is based in the United States.

28. Upon information and belief, SAIC and Samsung Research are both responsible for the development of Samsung's facial recognition technology and algorithms.

JURISDICTION AND VENUE

29. This Court has jurisdiction over the subject matter of this action pursuant to 28

U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative members of the Classes defined below, and a significant portion of putative Class members are citizens of a state different from at least one Defendant.

30. This Court has personal jurisdiction over Samsung because it regularly conducts business in Illinois and a substantial part of the harm, events, and conduct giving rise to Plaintiff's claims occurred in Illinois.

31. Venue is proper in this District pursuant to 28 U.S.C. §1391(b), (c), and (d) because Samsung transacts business in this District and a substantial portion of the events giving rise to the claims occurred in this District.

FACTUAL BACKGROUND

I. The risks posed by Biometrics.

32. The proliferation of behavioral economics and marketing science have caused a significant expansion in the use of Biometrics.

33. Biometrics are unique physical characteristics such as retina or iris scans, fingerprints, voiceprints, or hand and face geometry scans as well as the information based on or derived from it.

34. Each person has a unique facial geometry composed of various measures such as the distances between key facial landmarks and the ratios between those distances.

35. Biometrics are one of the most sensitive forms of personal information because biometric data cannot be changed once the data is stolen or compromised. Once a person's unique and permanent biometric identifiers are exposed, the victim is left with no recourse to prevent identity theft and/or unauthorized tracking.

36. The largest-ever-conducted study on the subject matter by the University of Texas titled *Consumer Attitudes About Biometric Authentication*, showed that 86%[3] of consumers were concerned about the misuse of their personal information and fewer than 10%[4] of consumers felt comfortable giving up their Biometrics for online shopping, internet games, or accessing online school records.

37. That same study revealed "invasion of personal privacy" is the chief reason for consumers' discomfort in sharing their Biometrics.[5] Similarly, a recent survey of 1,000 individuals published by digital identity firm Entrust titled *State of Consumer Data Privacy Survey*,[6] found 79% of respondents were concerned about their privacy, a fear mainly driven by the risks of attacks and security breaches.

38. One of the most prevalent uses of biometric identifiers is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific details about the face's geometry as determined by facial points and contours, and comparing the resulting "face template" (or "faceprint") to the face templates stored in a face template database. If a database match is found, an individual may be identified.

39. Once a picture of a person's face is scanned and its biometric measurements are captured, computers can store that information and use it to identify that individual any other time that person's face appears on the internet or in public using facial recognition.

---

[3] RACHEL L. GERMAN, ET AL., *Consumer Attitudes About Biometric Authentication* 24 (Univ. of Tex. At Austin Ctr. For Identity May 2018), https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf.

[4] *Id.* at 14.

[5] *Id.* at 15.

[6] Alessandro Mascellino, *Consumers' Contrasting Opinions Towards Biometric Adoption Shown by Entrust Report*, BIOMETRIC UPDATE (Feb. 1, 2021), https://www.biometricupdate.com/202102/consumers-contrasting-opinions-towards-biometric-adoption-shown-by-entrust-report.

40. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. Given the clear potential for misuse, the Federal Trade Commission ("FTC") urged companies using facial recognition technology and collecting biometric data to ask for clear consent before scanning and extracting biometric data from their digital photographs.

41. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[7] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[8]

42. Despite these efforts, there has been a significant exploitation of biometric data. For example, for eight years, RiteAid deployed facial recognition systems in largely lower-income, non-white neighborhoods, allegedly to target these demographics specifically.[9]

II. The Illinois Legislature enacts BIPA.

43. In the 2000's, major national corporations started using Chicago and other locations in Illinois to test new applications of biometric-facilitated transactions. *See* 740 ILCS 14/5(b).

44. In late 2007, a biometric company called Pay by Touch—which provided major retailers throughout the State of Illinois with biometric scanners to facilitate consumer

[7] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.judiciary.senate.gov/download/statement-of-franken-pdf (last visited Feb. 7, 2020).

[8] *Id.*

[9] Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, Reuters (July 28, 2020, 11 A.M. GMT) (https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois legislature because suddenly there was a serious risk that citizens' biometric records—which can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections. The bankruptcy also highlighted that many persons who used the biometric scanners were unaware that the scanners were transmitting their data to the now-bankrupt company, and that their biometric identifiers could then be sold to unknown third parties.

45. In 2008, Illinois enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276.

46. BIPA makes it unlawful for a company to collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or information unless the company first:

a) informs the subject in writing that a biometric identifier or information is being collected or stored;

b) informs the subject in writing of the specific purpose and length of term for which a biometric identifier or information is being collected, stored, and used; and

c) receives a written release executed by the subject of the biometric identifier or information.

740 ILCS 14/15(b).

47. The statute defines "biometric identifier" to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

48. The statute defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

49. In addition, BIPA regulates how companies must handle Illinois consumers' Biometrics. *See, e.g.*, 740 ILCS 14/15(c)–(d). For instance, under BIPA no private entity in possession of biometric identifiers or information may disclose or disseminate this data unless it receives the subject's consent. 740 ILCS 14/15(d). BIPA prohibits selling, leasing, trading, or otherwise profiting from a person's Biometrics, 740 ILCS 14/15(c), and requires that companies develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying Biometrics when the initial purpose for collecting such data has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. It also requires companies to permanently destroy the Biometrics within those time frames irrespective of whether they develop the written policy as required. 740 ILCS 14/15(a).

50. Under BIPA, "[a] prevailing party may recover for each violation: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate." 740 ILCS 14/20.

III. Samsung's systematically collects Biometrics.

51. Samsung Devices are manufactured and sold with the Gallery App pre-installed as the default photograph and video application.

52. According to Samsung:

> The Gallery app can connect to the Samsung Cloud, making it really easy to share your unforgettable moments across all of your devices. You can also create shared albums so that all of your loved ones can follow along with your adventures, no

matter where you are in the world.[10]

53. Each time a user takes or receives a photograph, Samsung uses its proprietary facial recognition technology to capture a scan of the face geometry of each face it detects, which Samsung stores at least ephemerally, accesses, and uses to create a face template which Samsung then stores, accesses, and uses each time a new photograph is added to the Device.

54. Through its software, Samsung automatically scans and analyzes each photograph added to a Device, assigns a tag based on the object, faces, or individuals detected, and saves it to the Gallery App. If a face is detected, Samsung's algorithm captures a scan of the person's unique facial geometry—such as the length, width, depth and location of various facial landmarks, including the mouth, chin, nose, ears, eyes, eyebrows, as well as the distances and spacing between those features—and stores it at least ephemerally.

55. Samsung through its software then accesses the stored scan of face geometry and uses it to create a unique digital representation of the face (*i.e.* the face template).[11]

56. Each face template is a distinct numerical representation of the unique shape and geometry of an individual's face, including the contours of, and distance between, unique facial landmarks and features. Each face templates is unique to an individual and can be used to identify them.

57. Samsung stores the face templates in a database that Samsung keeps at least in the solid state memory of the user's Samsung Device.

---

[10] *How do I use the Gallery app on my Galaxy device?* Samsung, https://www.samsung.com/uk/support/mobile-devices/how-do-i-use-the-gallery-app/ (last viewed October 14, 2022).

[11] *See* Patent No.: US 11,222,196 B2: Simultaneous Recognition of Facial Attributes and Identity in Organizing Photo Albums (Jan. 11, 2022) (describing how Samsung applies facial processing technology to recognize facial landmark features to identify and organize photograph and video albums based on modifying an efficient convolutional neural network (CNN) which extracts facial representations suitable for face identification and attribute (age, gender, ethnicity, emotion, etc.)).

58. Samsung uses these face templates to organize and group photos based upon the particular individuals who appear in the photos. Through its software, Samsung accomplishes this by accessing the face templates stored in its database, including those face templates Samsung creates using scans of face geometry it extracts from the photographs stored in the Devices contact list,[12] which typically includes the person's name, phone number and/or e-mail address.[13] Samsung then accesses and compares the previously-stored face templates against the newly-stored face template(s) to determine whether there is a match.

59. This is confirmed by Samsung's patents.[14] This process uses "face clustering," which analyzes each image for facial "landmarks," extracts those key facial features when found, and converts said data into "vectors," each of which is assigned a numerical value. Once the vectors have been assigned, a clustering engine analyzes the vectors to determine if similar values exist for the faces in other photos. The mathematical representation of the person's face created in this process is based on and specific to their facial geometry, and is used by Samsung to identify the

[12] *See* Patent No.: US 10,666,869 B2: Image Display Apparatus and Image Display Method (May 26, 2020) ("The control unit 150 may recognize the subject included in the captured image by comparing a face of the subject included in the captured image with a database. For example, ***the control unit 150 may recognize the subject included in the captured image within persons included in a contact list.****"*) (emphasis added).

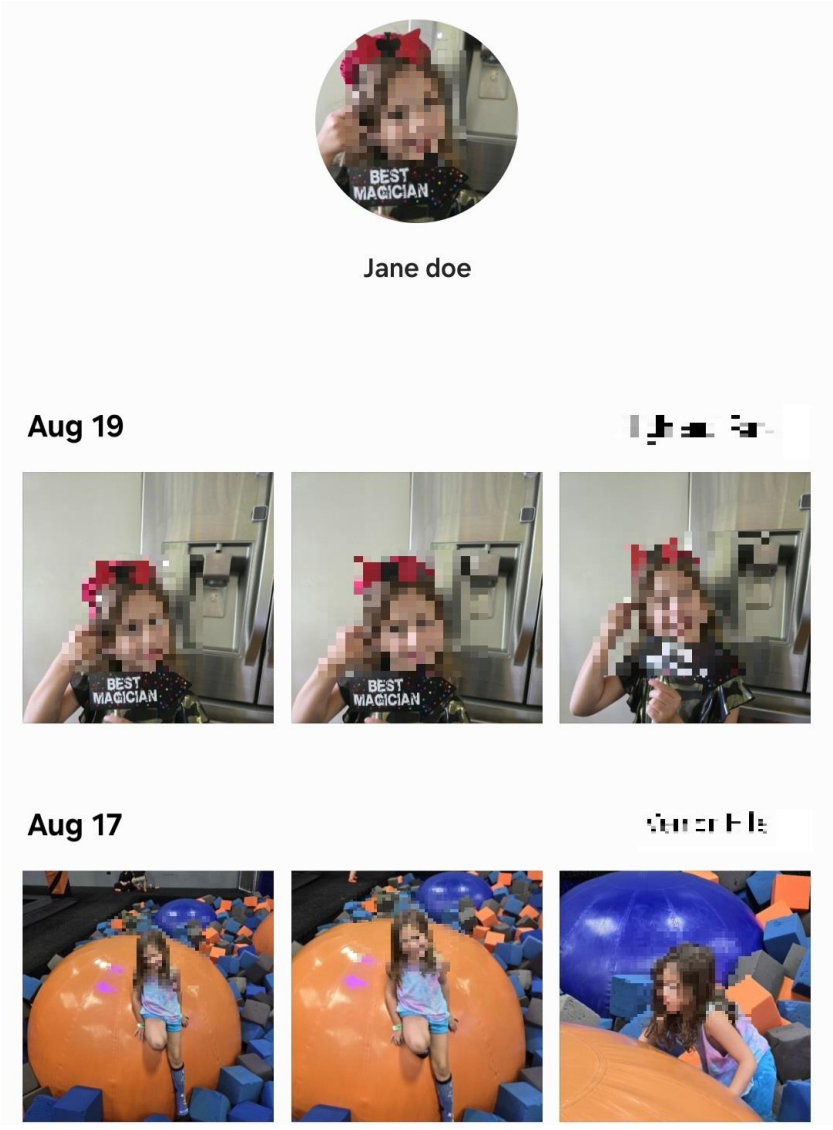
[13] *See Add a New Contact*, Samsung, https://www.samsung.com/us/support/answer/ANS00080368/ (last viewed August 20, 2024) (providing overview for adding contacts and stating "fill out their contact information and personal details. You can add multiple numbers and addresses the Phone and Email fields ….")

[14] *See* Patent No.: US 10,666,869 B2: Image Display Apparatus and Image Display Method (May 26, 2020) ("***[W]henever the image is captured, the control unit 150 may performed the face recognition on the captured image***. The control unit 150 may recognize the subject included in the captured image by comparing a face of the subject included in the captured image with a database. For example, the control unit 150 may recognize the subject included in the captured image within persons included in a contact list.") (emphasis added); *id.* ("The image display method may further include recognizing subjects included in the captured one or more images through face recognition, displaying tags corresponding to the recognized subjects and a share button on the camera preview screen, and sharing the captured one or more images in response to a touch input on the photo reel, at least one of the thumbnails, at least one of the tags, or the share button."); Patent No. US 10,129,481 B2: Image Display Apparatus and Image Display Method (Nov. 13, 2018) (same).

person in other photographs on the Device. Thus, the face templates constitute biometric information.

60. If there is a match, the Gallery App "tags" the image and groups it with previously stored images depicting the same individual. Images of the same individual are "stacked" together, with the front of the stack displaying the identified individual's face within a circular frame. If the user has "tagged" a photograph with the name of the depicted individual, that individual's name is shown below his or her face in the circular frame. (*See* Figure 1.)

(Figure 1)



61. As this process demonstrates, the biometric identifiers and biometric information Samsung captured, collected, and stored can be, and in fact were, used by Samsung to identify a specific individual, just as facial recognition identifies a specific individual as well as by name.

62. Through this process, Samsung systematically captures, collects, uses and stores the highly-sensitive Biometrics of each person whose face appears in a photograph stored on a Samsung Device — specifically, their unique facial geometry and face templates.

63. Consumers who buy Samsung Devices own the hardware, but merely license the software necessary for the device to function. That software is wholly owned and controlled by Samsung, as confirmed by Samsung's End User License Agreements ("EULAs"). The EULAs provide, in pertinent part:

> Samsung grants you a limited non-exclusive license to install, use, access, display and run one copy of the Samsung Software on a single Samsung Mobile Device[.] *** Samsung reserves all rights not expressly granted to you in this EULA. The Software is protected by copyright and other intellectual property laws and treaties. Samsung or its suppliers own the title, copyright and other intellectual property rights in the Samsung Software. The Samsung Software is licensed, not sold.

64. Under the terms of the EULAs, the Samsung Device user is prohibited from modifying or altering the software.

65. Because disabling facial recognition is not permitted by Samsung, the use of Samsung Devices to take or store photographs is conditioned on the collection of Biometrics.

66. Samsung indiscriminately collects Biometrics for all photographic subjects, including customers, non-customers, and minors incapable of providing informed consent.

67. The version of Samsung's Privacy Policy in effect when this case was filed expresly identifies "biometric information" as one category of personal information Samsung may collect. The Privacy Policy also lists additional categories of personal information Samsung may collect, including "identifiers such as a real name … postal address … telephone number ….email address

… and other similar identifiers."

68. Because Device users have no means of disabling the Samsung's facial recognition feature, the use of Samsung Devices to take or store photographs is conditioned on Samsung's capture and collection of Biometrics.

IV. Samsung has sole possession of the Biometrics collected by Samsung Devices.

69. Samsung has complete and exclusive control over the Biometrics it captured, collected and stored on Samsung Devices. To be clear, Samsung controls:

- Whether biometric identifiers or information are collected;
- What biometric identifiers or information are collected;
- The type of Biometrics that are collected and the format in which they are stored;
- The facial recognition algorithm that is used to collect Biometrics;
- What Biometrics are saved;
- Whether information based on biometric identifiers is used to identify users (thus creating biometric information);
- Whether Biometrics are kept locally on users' Samsung Devices;
- Whether Biometrics are encrypted or otherwise protected;
- Who can access the stored Biometrics; and
- How long Biometrics are stored.

70. Users of Samsung Devices, by contrast, have no ability to control the Biometrics Samsung captured and collected.

71. Users have no control over whether Samsung captures or collects Biometrics from their photo libraries, the location or manner in which their Biometrics are stored, or the manner in which their Biometrics are used or by whom.

72. Users cannot disable Samsung's capture or collection of Biometrics or limit what

information is captured or collected or from whom.

73. Users have no ability to access, use, or destroy their Biometrics that are collected and stored by Samsung.

74. Thus, Samsung fully controls—and thus possesses—the Biometrics on Samsung Devices.

75. Samsung's Gallery App has a feature that allows users to backup their photographs to a cloud server. Prior to September 2021, those photographs were uploaded and stored the Samsung Cloud, a cloud-server created, hosted, and controlled by Samsung.

V. Samsung's conduct violates BIPA.

76. Despite that BIPA was enacted nearly fifteen years ago, Samsung — a sophisticated commercial entity that is one of the world's leading manufacturers of smartphones and tablets — makes no effort to comply with the comprehensive regulatory regime imposed by the statute.

77. Samsung does not have a written, publicly-available policy establishing a retention schedule or guidelines for permanently destroying the biometric identifiers and biometric information it collects or otherwise obtains and does not permanently destroy the Biometrics it collects within the statutorily-mandated timeframes, in violation of BIPA § 15(a).

78. Samsung does not inform Illinois residents in writing that their biometric identifiers and biometric information are being captured, collected or stored before doing so, in violation of BIPA § 15(b)(1).

79. Samsung does not inform Illinois residents in writing of the specific purpose and length of time for which their biometric identifiers and information are being captured, collected, stored and used, or obtain a written release executed by each of those individuals, prior to capruing, collecting or otherwise obtaining their Biometrics, in violation of BIPA §§ 15(b)(2) and 15(b)(3).

80. Samsung's failure to comply with BIPA extends beyond just users of Samsung Devices to nonusers as well. This is because Samsung's Gallery App captures, collects and possesses the Biometric Data of everyone who appears in images stored in a user's photo library.

VI. Samsung's BIPA violations expose Plaintiffs and the other Class members to threats of serious harm.

81. Samsung does not delete the Biometrics it collects, which are located on numerous devices in this State.

82. Samsung Device users' as well as non-users' Biometrics may be stored on one or more Samsung Devices in use, as well as on discarded Samsung Devices.

83. Furthermore, non-users' Biometrics that Samsung collects may be stored on one or more Samsung Devices as well as on discarded Samsung Devices.

84. For example, an Illinois resident's Biometrics may be stored on his or her own Samsung Device(s) and/or on the Samsung Devices of his or her family members, relatives, friends, coworkers, and anyone else who photographed him or her using a Samsung Device or stored a photograph of him or her on a Samsung Device.

85. Information stored in a central location, such as a server, presents a single breach threat. A sophisticated entity may take measures to securely and centrally store information, guarding against the threat of a data breach. By contrast, as the result of the fact that the Biometrics Samsung collects are stored on numerous devices, Plaintiffs and members of the Class face the imminent threat of disclosure of their Biometrics as a result of a data breach on any one of the Samsung Devices on which their Biometrics are stored.

86. Samsung has nearly a 30% market share of the smartphone market in the United

States,[15] and a 17.6% marketshare of the tablet market.[16] 85% of adult Americans use smartphones, and 53% use tablets.[17]

87. Samsung developed the facial recognition feature of its Gallery App, in part, to compete with other electronic device vendors and software developers, and in order to sell Samsung Devices.

88. Many of the Samsung Devices used in this State have collected the Biometrics of multiple individuals other than the Samsung Device user. Consequently, numerous Illinois residents have their Biometrics stored on one or more Samsung Devices outside their control.

89. The durability of the memory in Samsung Devices creates a near-permanent risk of a data breach of biometric identifiers and information for both device users as well as nonusers whose Biometrics have been collected. Samsung Devices utilize solid state memory, which can withstand drops, extreme temperatures, and magnetic fields.[18] Unless corrupted, this solid state memory and the information it contains can last in perpetuity. Thus, the Biometrics on Samsung Devices will likely outlast the device battery, the functionality of the device screen, and the natural life of the device user.

90. Biometrics may persist on discarded Samsung Devices, which could be extracted by malicious actors using methods of removal that may or may not currently exist.[19] The risk of

---

[15] Chance Miller, *Canalys: Apple Shipped 14.6M iPhones in North America During Ql, Securing 40% Marketshare,* 9to5Mac (May 9, 2019 3:23 PM), https://9to5mac.com/2019/05/09/iphone-north-america-marketshare/.

[16] Tablet Vendor Market Share United States of America (June 2021), *available at* https://gs.statcounter.com/vendor-market-share/tablet/united-states-of-america.

[17] *Mobile Fact Sheet,* Pew Research Center (Apr. 7, 2021), *available at* https://www.pewresearch.org/ internet/fact-sheet/mobile/.

[18] Roderick Bauer, *SSD 101: How Reliable are SSDs?,* BackBlaze (Feb. 21, 2019), https://www.backblaze.com/blog/how-reliable-are-ssds/.

[19] *See, e.g.*, Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech,* Rapid7 Blog (Mar. 19, 2019), https://www.rapid7.com/blog/post/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/; Federal Trade Commission, *How to Protect Your Phone and the Data On It*, https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-

illicit harvesting of Biometrics from discarded Samsung Devices therefore extends far into the future.

91. This risk is not merely hypothetical. Following a recent cyberattack on Samsung, a notorious hacker collective leaked a trove of source code related to all recent Samsung Devices, including the source code for biometric authentication and on-device encryption.[20]

VII. Plaintiffs' experiences with Samsung Devices.

Plaintiff G.T.

92. Plaintiff G.T. is a fourteen year-old minor. She previously owned Samsung Galaxy A20, which she used to take photos of herself and other people while residing in the State of Illinois.

93. Plaintiff G.T. has an Instagram account that is searchable by her name and features a publicly-available account photo of her face.

94. Plaintiff G.T. also appears in photographs on her relatives' Samsung Devices.

95. Each time Plaintiff G.T. took a photograph of herself or others, Samsung collected, captured, received through trade, or otherwise obtained the Biometrics — specifically, the facial geometry and face prints — of everyone whose face appeared on the photograph.

96. Plaintiff G.T. has not—and cannot—give consent for Samsung to collect or possess her biometric identifiers and biometric information. Further, Plaintiff G.T.'s parents have not given prior informed written consent for Samsung to collect or possess G.T.'s biometric identifiers and biometric information.

---

it (last visited August 4, 2021); William Gallagher, *Wipe Your iPhone Before Selling It, Because If You Don't You Might Get Your Data Stolen*, Apple Insider (Jul 26, 2018), https://appleinsider.com/articles/18/07/26/wipe-your-iphone-before-selling-it-because-if-you-dont-you-might-get-your-data-stolen.

[20] *See* I. Bonifacic, *Hackers may have obtained 190GB of sensitive data from Samsung*, Engadget (March 15, 2022), https://www.engadget.com/samsung-lapsus-leak-181517961.html.

97. Plaintiff G.T. was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on facial geometry. Samsung's facial recognition technology collected biometric identifiers and information (*e.g.* scans of facial geometry, face templates) not only from Plaintiff G.T., but also from other individuals appearing in photographs on Plaintiff G.T.'s Samsung Device, including parents, siblings (who are minors), cousins (some of whom are minors), and a grandparent of Plaintiff G.T.

98. The Gallery App on Plaintiff G.T.'s Samsung Device automatically compared the face templates of individuals who appear in newly-stored photos on her device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

99. Samsung's facial recognition technology also collected biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of Plaintiff G.T. stored in the photo libraries of other peoples' Samsung Devices, including her relatives' Samsung Devices.

100. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff G.T. in the photo library automatically compared the face templates of Plaintiff G.T. and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

101. At all relevant times, Plaintiff G.T. was unaware of Samsung's facial recognition "feature" of the Gallery App.

102. Samsung has not informed Plaintiff G.T. that Biometrics have been and are being collected from the individuals whose faces appear in photographs stored in her Samsung Device.

103. Moreover, Samsung has not informed Plaintiff G.T. that the Gallery App is installed

on her device by default and will operate on mobile devices whenever a photograph is added to the photo library.

104. Samsung did not obtain consent from Plaintiff G.T. in any form prior to harvesting her Biometrics, let alone the written, informed consent required by BIPA.

105. Samsung never provided Plaintiff G.T. with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and biometric information.

106. By collecting Plaintiff G.T.'s unique biometric identifiers and biometric information without her consent, written or otherwise, Samsung invaded her statutorily protected right to privacy in her Biometrics.

107. Further, Samsung never provided Plaintiff G.T. with a retention schedule or guidelines for permanently destroying her biometric identifiers and biometric information.

108. Samsung's acts and omissions denied Plaintiff G.T. the opportunity to consider whether the terms of Samsung's collection, storage, and usage of her biometric identifiers and biometric information were acceptable given the attendant risks, and denied her the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed her concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff Jones

109. Plaintiff Jones has owned a Samsung Galaxy device since at least 2018, which she used to take photos of herself and other people while residing in the State of Illinois.

110. Each time Plaintiff Jones took a photograph of herself or others, Samsung collected, captured, received through trade, or otherwise obtained the Biometrics — specifically, the facial geometry and face prints — of everyone whose face appeared on the photograph.

111. Plaintiff Jones was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on facial geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of facial geometry, face templates) not only from Plaintiff Jones, but also from other individuals appearing in photographs on Plaintiff's Samsung Device.

112. The Gallery App on Plaintiff Jones's Samsung Device automatically compared the face templates of individuals who appear in newly-stored photos on her device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

113. Samsung's facial recognition technology also collected biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of Plaintiff Jones stored in the photo libraries of other peoples' Samsung Devices.

114. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff Jones in the photo library automatically compared the face templates of Plaintiff Jones and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

115. At all relevant times, Plaintiff Jones was unaware of Samsung's facial recognition "feature" of the Gallery App.

116. Samsung has not informed Plaintiff Jones that Biometrics have been and are being collected from the individuals whose faces appear in photographs stored in her Samsung Device.

117. Moreover, Samsung has not informed Plaintiff Jones that the Gallery App is installed on her device by default and will operate on mobile devices whenever a photograph is

added to the photo library.

118. Samsung did not obtain consent from Plaintiff Jones in any form prior to harvesting her Biometrics, let alone the written, informed consent required by BIPA.

119. Samsung never provided Plaintiff Jones with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and biometric information.

120. By collecting Plaintiff Jones's unique biometric identifiers and biometric information without her consent, written or otherwise, Samsung invaded her statutorily protected right to privacy in her Biometrics.

121. Further, Samsung never provided Plaintiff Jones with a retention schedule or guidelines for permanently destroying her biometric identifiers and biometric information.

122. Samsung's acts and omissions denied Plaintiff Jones the opportunity to consider whether the terms of Samsung's collection, storage, and usage of her biometric identifiers and biometric information were acceptable given the attendant risks, and denied her the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed her concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff DeMatteo

123. Plaintiff DeMatteo currently owns a Samsung Galaxy S20 FE phone, and previously owned a Samsung Galaxy S8 Plus, both of which he has used to take photos of himself.

124. Plaintiff DeMatteo has a Facebook account that is searchable by his name and features a publicly-available account photo of his face.

125. Plaintiff DeMatteo also appears in photographs on the Samsung Devices of his relatives, friends, and others.

126. Plaintiff DeMatteo did not give consent for Samsung to collect, capture, obtain, or possess his biometric identifiers and biometric information.

127. Plaintiff DeMatteo was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of face geometry, face templates) not only from Plaintiff DeMatteo, but also from other individuals appearing in photographs on Plaintiff DeMatteo's Samsung Device.

128. The Gallery App on Plaintiff DeMatteo's Samsung Devices automatically compared the face templates of individuals who appear in newly-stored photos on his device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

129. Samsung's facial recognition technology also collected Plaintiff DeMatteo's biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of him stored in the photo libraries of other peoples' Samsung Devices, including his relatives' and friends' Samsung Devices.

130. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff DeMatteo in the photo library automatically compared the face templates of Plaintiff DeMatteo and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

131. At all relevant times, Plaintiff DeMatteo was unaware of Samsung's facial recognition "feature" of the Gallery App.

132. Samsung did not inform Plaintiff DeMatteo that Biometrics were and are being

collected from the individuals whose faces appear in photographs stored in his Samsung Devices.

133. Moreover, Samsung has not informed Plaintiff DeMatteo that the Gallery App is installed on his device by default and will operate on mobile devices whenever a photograph is added to the photo library.

134. Samsung did not obtain Plaintiff DeMatteo's informed written consent, as required by BIPA, prior to harvesting his Biometrics.

135. Samsung never provided Plaintiff DeMatteo with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of his unique biometric identifiers and biometric information.

136. By collecting Plaintiff DeMatteo's unique biometric identifiers and biometric information without his consent, written or otherwise, Samsung invaded his statutorily-protected right to privacy in his Biometrics.

137. Further, Samsung never provided Plaintiff DeMatteo with a retention schedule or guidelines for permanently destroying his biometric identifiers and biometric information.

138. Samsung's acts and omissions denied Plaintiff DeMatteo the opportunity to consider whether the terms of Samsung's collection, storage, and usage of his biometric identifiers and biometric information were acceptable given the attendant risks, and denied him the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed his concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff Jacobs

139. Plaintiff Jacobs owns a Samsung Galaxy A20 phone, which he has used to take photos of himself.

140. Plaintiff Jacobs also appears in photographs on the Samsung Devices of his

relatives, friends, and others.

141. Plaintiff Jacobs did not give consent for Samsung to collect, capture, obtain, or possess his biometric identifiers and biometric information.

142. Plaintiff Jacobs was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of face geometry, face templates) not only from Plaintiff Jacobs, but also from other individuals appearing in photographs on Plaintiff Jacobs's Samsung Device.

143. The Gallery App on Plaintiff Jacobs's Samsung Device automatically compared the face templates of individuals who appear in newly-stored photos on his device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

144. Samsung's facial recognition technology also collected Plaintiff Jacobs's biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of him stored in the photo libraries of other peoples' Samsung Devices, including his relatives' and friends' Samsung Devices.

145. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff Jacobs in the photo library automatically compared the face templates of Plaintiff Jacobs and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

146. At all relevant times, Plaintiff Jacobs was unaware of Samsung's facial recognition "feature" of the Gallery App.

147. Samsung did not inform Plaintiff Jacobs that Biometrics were and are being collected from the individuals whose faces appear in photographs stored in his Samsung Devices.

148. Moreover, Samsung has not informed Plaintiff Jacobs that the Gallery App is installed on his device by default and will operate on mobile devices whenever a photograph is added to the photo library.

149. Samsung did not obtain Plaintiff Jacobs's informed written consent, as required by BIPA, prior to harvesting his Biometrics.

150. Samsung never provided Plaintiff Jacobs with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of his unique biometric identifiers and biometric information.

151. By collecting Plaintiff Jacobs's unique biometric identifiers and biometric information without his consent, written or otherwise, Samsung invaded his statutorily-protected right to privacy in his Biometrics.

152. Further, Samsung never provided Plaintiff Jacobs with a retention schedule or guidelines for permanently destroying his biometric identifiers and biometric information.

153. Samsung's acts and omissions denied Plaintiff Jacobs the opportunity to consider whether the terms of Samsung's collection, storage, and usage of his biometric identifiers and biometric information were acceptable given the attendant risks, and denied him the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed his concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff Cosby-Steel

154. Plaintiff Cosby-Steel owns a Samsung Galaxy A13 phone, and previously owned a Samsung Note 20 phone, both of which she has used to take photos of herself.

155. Plaintiff Cosby-Steel has Facebook and Instagram accounts that are searchable by her name and feature publicly-available photos of her face.

156. Plaintiff Cosby-Steel also appears in photographs on the Samsung Devices of her relatives, friends, and others.

157. Plaintiff Cosby-Steel did not give consent for Samsung to collect, capture, obtain, or possess her biometric identifiers and biometric information.

158. Plaintiff Cosby-Steel was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of face geometry, face templates) not only from Plaintiff Cosby-Steel, but also from other individuals appearing in photographs on Plaintiff Cosby-Steel's Samsung Devices.

159. The Gallery App on Plaintiff Cosby-Steel's Samsung Devices automatically compared the face templates of individuals who appear in newly-stored photos on her device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

160. Samsung's facial recognition technology also collected Plaintiff Cosby-Steel's biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of her stored in the photo libraries of other peoples' Samsung Devices, including her relatives' and friends' Samsung Devices.

161. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff Cosby-Steel in the photo library automatically compared the face templates of Plaintiff Cosby-Steel and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with

previously-stored photos depicting the same individuals.

162. At all relevant times, Plaintiff Cosby-Steel was unaware of Samsung's facial recognition "feature" of the Gallery App.

163. Samsung did not inform Plaintiff Cosby-Steel that Biometrics were and are being collected from the individuals whose faces appear in photographs stored in her Samsung Devices.

164. Moreover, Samsung has not informed Plaintiff Cosby-Steel that the Gallery App is installed on her device by default and will operate on mobile devices whenever a photograph is added to the photo library.

165. Samsung did not obtain Plaintiff Cosby-Steel's informed written consent, as required by BIPA, prior to harvesting her Biometrics.

166. Samsung never provided Plaintiff Cosby-Steel with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and biometric information.

167. By collecting Plaintiff Cosby-Steel's unique biometric identifiers and biometric information without her consent, written or otherwise, Samsung invaded her statutorily-protected right to privacy in her Biometrics.

168. Further, Samsung never provided Plaintiff Cosby-Steel with a retention schedule or guidelines for permanently destroying her biometric identifiers and biometric information.

169. Samsung's acts and omissions denied Plaintiff Cosby-Steel the opportunity to consider whether the terms of Samsung's collection, storage, and usage of her biometric identifiers and biometric information were acceptable given the attendant risks, and denied her the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed her concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff Maday

170. Plaintiff Maday owned a Samsung Galaxy S8 from 2016 through approximately October 2018, and owned a Galaxy S9 from approximately November 2018 until in or around December 2020, both which he used to take photos of himself.

171. Plaintiff Maday has Instagram and LinkedIn accounts that are searchable by his name, and each account features one or more publicly-available photos of his face.

172. Plaintiff Maday also appears in photographs on other peoples' Samsung Devices.

173. Plaintiff Maday did not give consent for Samsung to collect, capture, obtain, or possess his biometric identifiers and biometric information.

174. Plaintiff Maday was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of face geometry, face templates) not only from Plaintiff Maday, but also from other individuals appearing in photographs on Plaintiff Maday's Samsung Devices.

175. The Gallery App on Plaintiff Maday's Samsung Devices automatically compared the face templates of individuals who appear in newly-stored photos on his device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

176. Samsung's facial recognition technology also collected Plaintiff Maday's biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of him stored in the photo libraries of other peoples' Samsung Devices.

177. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff Maday in the photo library automatically compared the face templates of Plaintiff Maday

and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

178. At all relevant times, Plaintiff Maday was unaware of Samsung's facial recognition "feature" of the Gallery App, though he has "tagged" individuals in photographs that Samsung has organized by facial geometry.

179. Samsung did not inform Plaintiff Maday that Biometrics were and are being collected from the individuals whose faces appear in photographs stored in his Samsung Devices.

180. Moreover, Samsung has not informed Plaintiff Maday that the Gallery App is installed on his device by default and will operate on mobile devices whenever a photograph is added to the photo library.

181. Samsung did not obtain Plaintiff Maday's written, informed consent as required by BIPA prior to harvesting Plaintiff Maday's Biometrics.

182. Samsung never provided Plaintiff Maday with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of his unique biometric identifiers and biometric information.

183. By collecting Plaintiff Maday's unique biometric identifiers and biometric information without his consent, written or otherwise, Samsung invaded his statutorily-protected right to privacy in his Biometrics.

184. Further, Samsung never provided Plaintiff Maday with a retention schedule or guidelines for permanently destroying his biometric identifiers and biometric information.

185. Samsung's acts and omissions denied Plaintiff Maday the opportunity to consider whether the terms of Samsung's collection, storage, and usage of his biometric identifiers and

biometric information were acceptable given the attendant risks, and denied him the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed his concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff Thurman

186. Plaintiff Thurman owns a Samsung Galaxy S10 from approximately April 2018 through April 2022, and owned a Samsung Galaxy S22 from April 2022 through October 2022, both of which she has used to take photos of herself.

187. Plaintiff Thurman also appears in photographs on the Samsung Devices of her relatives, friends, and others.

188. Plaintiff Thurman did not give consent for Samsung to collect, capture, obtain, or possess her biometric identifiers and biometric information.

189. Plaintiff Thurman was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of face geometry, face templates) not only from Plaintiff Thurman, but also from other individuals appearing in photographs on Plaintiff Thurman's Samsung Devices.

190. The Gallery App on Plaintiff Thurman's Samsung Devices automatically compared the face templates of individuals who appear in newly-stored photos on her device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

191. Samsung's facial recognition technology also collected Plaintiff Thurman's biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of her stored in the photo libraries of other peoples' Samsung Devices, including her relatives' and

friends' Samsung Devices.

192. The Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff Thurman in the photo library automatically compared the face templates of Plaintiff Thurman and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

193. At all relevant times, Plaintiff Thurman was unaware of Samsung's facial recognition "feature" of the Gallery App.

194. Samsung did not inform Plaintiff Thurman that Biometrics were and are being collected from the individuals whose faces appear in photographs stored in her Samsung Devices.

195. Moreover, Samsung has not informed Plaintiff Thurman that the Gallery App is installed on her device by default and will operate on mobile devices whenever a photograph is added to the photo library.

196. Samsung did not obtain Plaintiff Thurman's informed written consent, as required by BIPA, prior to harvesting her Biometrics.

197. Samsung never provided Plaintiff Thurman with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and biometric information.

198. By collecting Plaintiff Thurman's unique biometric identifiers and biometric information without her consent, written or otherwise, Samsung invaded her statutorily-protected right to privacy in her Biometrics.

199. Further, Samsung never provided Plaintiff Thurman with a retention schedule or guidelines for permanently destroying her biometric identifiers and biometric information.

200. Samsung's acts and omissions denied Plaintiff Thurman the opportunity to consider whether the terms of Samsung's collection, storage, and usage of her biometric identifiers and biometric information were acceptable given the attendant risks, and denied her the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed her concrete interests that the legislature sought to protect by enacting BIPA.

Plaintiff Harris

201. Plaintiff Harris currently owns a Samsung Galaxy 21 phone, and prior to that owned a Samsung Galaxy S9 phone, both of which she has used to take photos of herself.

202. Plaintiff Harris has a Facebook account that is searchable by her name and features publicly-available photos of her face.

203. Plaintiff Harris also appears in photographs on the Samsung Devices of her relatives, friends, and others.

204. Plaintiff Harris did not give consent for Samsung to collect, capture, obtain, or possess her biometric identifiers and biometric information.

205. Plaintiff Harris was not aware Samsung's facial recognition technology would collect Biometrics and organize photos based on face geometry. Samsung's facial recognition technology collected biometric identifiers and information (e.g. scans of face geometry, face templates) not only from Plaintiff Harris, but also from other individuals appearing in photographs on Plaintiff Harris's Samsung Devices.

206. The Gallery App on Plaintiff Harris's Samsung Devices automatically compared the face templates of individuals who appear in newly-stored photos on her device to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

207. Samsung's facial recognition technology also collected Plaintiff Harris's biometric identifiers and information (e.g. scans of face geometry, face templates) from photos of her stored in the photo libraries of other peoples' Samsung Devices, including her relatives' and friends' Samsung Devices.

208. Upon information and belief, the Gallery App on other peoples' Samsung Devices that contain photos of Plaintiff Harris in the photo library automatically compared the face templates of Plaintiff Harris and other individuals who appear in newly-stored photos on those devices to face templates already saved in the facial database and grouped the newly-stored photos with previously-stored photos depicting the same individuals.

209. At all relevant times, Plaintiff Harris was unaware of Samsung's facial recognition "feature" of the Gallery App.

210. Samsung did not inform Plaintiff Harris that Biometrics were and are being collected from the individuals whose faces appear in photographs stored in her Samsung Devices.

211. Moreover, Samsung has not informed Plaintiff Harris that the Gallery App is installed on her device by default and will operate on mobile devices whenever a photograph is added to the photo library.

212. Samsung did not obtain Plaintiff Harris's informed written consent, as required by BIPA, prior to harvesting her Biometrics.

213. Samsung never provided Plaintiff Harris with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and biometric information.

214. By collecting Plaintiff Harris's unique biometric identifiers and biometric information without her consent, written or otherwise, Samsung invaded her statutorily-protected

right to privacy in her Biometrics.

215. Further, Samsung never provided Plaintiff Harris with a retention schedule or guidelines for permanently destroying her biometric identifiers and biometric information.

216. Samsung's acts and omissions denied Plaintiff Harris the opportunity to consider whether the terms of Samsung's collection, storage, and usage of her biometric identifiers and biometric information were acceptable given the attendant risks, and denied her the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed her concrete interests that the legislature sought to protect by enacting BIPA.

CLASS ALLEGATIONS

217. **Class Definition**. Plaintiffs bring this action on behalf of a class of all similarly-situated individuals (the "Class") that is defined, subject to amendment, as follows:

> All individuals who, while residing in the State of Illinois, had their biometric identifiers or biometric information collected, captured, received or otherwise obtained and/or stored by Samsung.

218. Plaintiffs represent and are members of the Class. Excluded from the Class are Samsung and any entities in which Samsung has a controlling interest, Samsung's employees and agents, the Judge to whom this action is assigned, and any member of the Judge's staff and immediate family.

219. Certification of Plaintiffs' claim for classwide treatment is appropriate because Plaintiffs can prove the elements of their claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

220. **Numerosity**. The number of persons within the Class is substantial, and is reasonably believed to include thousands of persons as Samsung has nearly 30% of the smartphone market in the United States and 17.6% of the tablet market, having sold more than two billion

Galaxy smartphones sold since 2009 and over 50 million Galaxy Tab tablets in the past two years alone. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. While the exact number of Class member is currently unknown, this information can be ascertained from Samsung's and third-parties' records. Class members can be notified about the pendency of this action through recognized, Court-approved methods of notice dissemination, such as U.S. Mail, electronic mail, internet postings, and/or published notice.

221. **Commonality and Predominance.** This action involves common questions of law and fact, which predominate over any questions affecting Class members, including, without limitation:

(a) whether Samsung collected or otherwise obtained the Class members' biometric identifiers or biometric information;

(b) whether Samsung possessed the Class members' biometric identifiers or biometric information;

(c) whether Samsung informed the Class members in writing that their biometric identifiers and biometric information are being collected or stored;

(d) whether Samsung informed Class members in writing of the specific purposes and length of term for which their biometric identifiers and biometric information are being collected, stored, and used;

(e) whether Samsung received a signed written release (as defined in 740 ILCS 14/10) to collect, use, and store the Class members' biometric identifiers and biometric information;

(f) whether Samsung maintained a publicly-available written policy establishing a retention schedule and guidelines for the destruction of biometric identifiers and information at the time it collected the Class members' biometric identifiers and biometric information;

(g) whether Samsung complied with any such written policy;

(h) whether Samsung permanently destroyed the Class members' biometric identifiers and biometric information;

(i) whether Samsung used the Class members' biometric identifiers or biometric information to identify them;

(j) whether Samsung violated BIPA; and

(k) whether Samsung's violations of BIPA were negligent, reckless, or intentional.

222. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex and class action litigation. Plaintiffs have no interests antagonistic to those of the Class.

223. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

COUNT I
Violation of 740 ILCS 14/15(a)
(On Behalf of Plaintiffs and the Class)

224. Plaintiffs restate and re-allege all paragraphs of this Complaint as though fully set forth herein.

225. BIPA requires private entities in possession of Biometrics to establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, those entities must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent destruction of biometric data (at most three years after the entity's last interaction with the individual); and (ii) adhere to that retention schedule and actually delete the biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

226. Samsung failed to comply with either of these BIPA mandates.

227. Samsung is a company registered to do business in Illinois, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

228. Plaintiffs and the Class members are individuals whose biometric identifiers and/or biometric information are possessed by Samsung.

229. Samsung violated BIPA by not maintaining the statutorily-mandated retention schedule and destruction guidelines at the time it collected Plaintiffs' and the Class member's biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

230. Samsung violated BIPA by failing to permanently destroy Plaintiffs' and the Class members' biometric identifiers and biometric information as required. *See* 740 ILCS 14/15(a).

231. By failing to destroy Plaintiffs' and the Class members' biometric identifiers and biometric information, Samsung unlawfully retained their Biometrics.

232. Samsung's conduct intentionally or recklessly violated BIPA with respect to

Plaintiffs and the Class members.

233. In the alternative, Samsung's conduct negligently violated BIPA with respect to Plaintiffs and the Class members.

234. Accordingly, Plaintiffs, on behalf of themselves and the Class, seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Samsung to immediately and permanently destroy their biometric identifiers and biometric information, and to comply with BIPA's requirements that private entities maintain and comply with publicly-available guidelines for permanently destroying biometric identifiers and biometric information; (3) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorney's fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II
Violation of 740 ILCS 14/15(b)
(On Behalf of Plaintiffs and the Class)

235. Plaintiffs restate and re-allege all paragraphs of this Complaint as though fully set forth herein.

236. BIPA requires private entities such as Samsung to obtain informed written consent from individuals before acquiring their Biometrics. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's . . . biometric identifier or biometric information, unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; **and** (3) receives a written

release executed by the subject of the biometric identifier or biometric information . . . .” 740 ILCS 14/15(b).

237. Samsung is a company registered to do business in Illinois, and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

238. Plaintiffs and the Class members are individuals whose “biometric identifiers” and “biometric information,” as defined by the BIPA—including, without limitation, scans of their facial geometry and face templates—were collected or otherwise obtained, stored, and used by Samsung.

239. Samsung violated BIPA by failing to inform Plaintiffs and the Class, in writing, about the collection and storage of their biometric identifiers and biometric information before it occurred. *See* 740 ILCS 14/15(b)(1).

240. Samsung violated BIPA by failing to inform Plaintiffs and the Class, in writing before the fact, of the specific purpose and length of term for which their biometric identifiers and biometric information were being “collected, stored, and used” before it occurred. *See* 740 ILCS 14/15(b)(2).

241. Samsung violated BIPA by collecting, capturing, purchasing, receiving through trade, and otherwise obtaining Plaintiffs’ and the Class members’ biometric identifiers and biometric information without first obtaining a signed written release from each of them. *See* 740 ILCS 14/15(b)(3).

242. In so doing, Samsung deprived Plaintiffs and the Class of their statutory right to maintain the privacy of their biometric identifiers and biometric information.

243. Samsung’s conduct intentionally or recklessly violated BIPA with respect to Plaintiffs and the Class members.

244. In the alternative, Samsung's conduct negligently violated BIPA with respect to Plaintiffs and the Class members.

245. Accordingly, Plaintiffs, on behalf of themselves and the Class, seeks: (1) declaratory relief; (2) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); (3) injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Samsung to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information, as described herein; and (4) reasonable attorney's fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff G.T. (by and through her next friend Liliana T. Hanlon), Plaintiff Jones, Plaintiff Jacobs, Plaintiff DeMatteo, Plaintiff Maday, Plaintiff Cosby-Steel, Plaintiff Thurman, and Plaintiff Harris, on behalf of themselves and the proposed Class, respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above (or on behalf of any other class the Court deems appropriate);

B. Appointing Plaintiffs as representatives of the Class, and their undersigned attorneys as class counsel;

C. Declaring that Samsung's acts and omissions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;

D. Awarding statutory damages of $5,000 for each and every intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000

for each and every negligent violation pursuant to 740 ILCS 14/20(1) if the Court finds that Samsung's violations were negligent;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including, *inter alia*, requiring Samsung to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information, and to permanently destroy Plaintiffs' and the Class members' biometric identifiers and biometric information;

F. Awarding Plaintiffs and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiffs and the Class members pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiffs, individually and on behalf of all others similarly situated, hereby demand a trial by jury on all issues so triable.

Dated: August 21, 2024

Respectfully submitted,

G.T., BY AND THROUGH NEXT FRIEND LILIANA T. HANLON, SHIMERA JONES, LEROY JACOBS, BALARIE COSBY-STEELE, JOHN DEMATTEO, RICHARD MADAY, ALLISON THURMAN, AND SHERIE HARRIS, individually and on behalf of all others similarly situated, Plaintiffs

By: /s/ Gregg M. Barbakoff

Keith J. Keogh
Theodore H. Kuyper
Gregg M. Barbakoff
KEOGH LAW, LTD.
55 W. Monroe Street, Suite 3390
Chicago, Illinois 60603
(312) 726-1092
keith@keoghlaw.com
tkuyper@keoghlaw.com
gbarbakoff@keoghlaw.com

Christian Levis (*pro hac vice forthcoming*)
Amanda Fiorilla (*pro hac vice forthcoming*)
Rachel Kesten (*pro hac vice forthcoming*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com

Attorneys for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that, on August 21, 2024, I caused a copy of the foregoing ***Consolidated Second Amended Class Action Complaint*** to be served upon all counsel of record via electronic filing using the CM/ECF system.

/s/ Gregg M. Barbakoff